25 junio de 2024

Salario Mínimo	INPC May.	UMA Diario	Recargo Por Mora	Tipo de Cambio	UDIS
207.44	134.08	108.57	1.65%	18.18	8.1225

IDENTIFIQUE CORREOS APÓCRIFOS

En últimas fechas hemos recibido muchísimos correos que pueden ser apócrifos, y que nos hemos dado a la tarea de identificarlos como como puntos finos de tal suerte que **IDENTIFIQUE previamente si es un correo para robarle su identidad o peor aún que hagan acopio de su información y posteriormente les llamen para pedir un rescate para devolvérsela.**

1. No descargar archivos o hacer clic en enlaces.
2. Desconfiar de correos que pidan descargar archivos o abrir vínculos, debido a que delincuentes cibernéticos suelen incluir estos en los correos falsos, con el objetivo de instalar software malicioso, asimismo, archivos falsos a nombre de las instituciones.
3. Confirmar dirección. Puede ser obvio, pero se debe confirmar que la dirección de correo electrónico del remitente coincida con la entidad que afirma ser, ya que los delincuentes cibernéticos utilizan nombres casi idénticos a los legítimos. El correo electrónico puede mostrar que proviene por ejemplo de North Bank, pero la dirección del remitente puede ser un tanto extraña, como northbank@hotmail.com. El remitente no utilizará una cuenta de Internet pública como Hotmail, Gmail o Yahoo! si la intención es ser una empresa legítima.
4. Verificar ortografía. Los mensajes fraudulentos suelen contener errores gramaticales que las entidades oficiales nunca incluirían en un mensaje para sus destinatarios.
5. No enviar datos personales.
6. Desconfiar de correos que requieran hacer actualizaciones de datos.
7. Verificar cuentas o que soliciten contraseñas privadas.
8. También verificar imágenes. Los correos electrónicos falsos suelen incluir imágenes o logotipos de instituciones, para engañar fácilmente a los destinatarios, en este sentido, hay que verificar que las imágenes no estén distorsionadas o borrosas
9. Si usa una computadora, pase el ratón por el enlace para obtener una vista previa de la URL del enlace en la barra de estado. A continuación, compruebe si el enlace del sitio es igual al URL legítimo. De esta manera, por ejemplo, si recibe un correo electrónico de “North Bank” y el enlace no va a www.northbank.com, sino a un sitio como www.banking-north.com, no haga clic.
10. Si usa un dispositivo móvil, utilice la vista previa del enlace para ver la URL real antes de hacer clic.

11. Compruebe si la dirección web comienza con “https” en vez de “http”, ya que este es un indicio de que la página web es segura.
12. Compruebe el saludo. Si el mensaje comienza con “Estimado(a) Sr./Sra.” o “Apreciado(a) cliente”, puede parecer sospechoso. Por lo general, los remitentes con los que tiene una relación lo llamarán por su nombre.
13. Busque imágenes de baja resolución y errores ortográficos. Los errores ortográficos o gramaticales son otra señal segura de que el mensaje o sitio es falso. Otra pista es la mala calidad de imagen del logotipo de la empresa u otros gráficos.
14. Si recibe una solicitud mediante correo electrónico por parte de alguien que conoce que le pide información confidencial y parece provenir de una dirección de correo electrónico real, sepa que puede tratarse de un caso de falsificación de correo electrónico. Hable con la persona directamente para confirmar si realmente envió la solicitud mediante correo electrónico.
15. Recuerde instalar en su computadora un buen antivirus.

SI SOSPECHA QUE ES UN CORREO APROCRIFO, NO LO ABRA NI LO REENVIE, por favor SOLO ELIMINELO

Sóstenes Rocha N.12
Col.Tamborrel
Xalapa, Veracruz.
(228) 818 05 83
228 108 3847
Contacto@palafox.mx
www.palafox.mx

José Manuel Garma
manuel.garma@palafox.mx

Juan Daniel Garma
daniel.garma@palafox.mx

Josefina Palafox Centurión
direccion@palafox.mx